UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,092	10/03/2003	David Andrew Thomas	200309084-1	3543

22879 7590 03/02/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
03/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/679,092
Filing Date: October 03, 2003
Appellant(s): THOMAS ET AL.

Ashok K. Mannava
Reg. No. 45,301
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04 November 2008 appealing from the Office action mailed 06 June 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejections of claims 11, 21, and 27-29 under 35 U.S.C. 103(a) have been withdrawn.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,385,596	WISER	5-2002
2002/0064283	PARENTY	5-2002
2002/0027994	KATAYAMA	3-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-10, 12-17, 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser, U.S. Patent No. 6,385,596, in view of Parenty, U.S. Publication No. 2002/0064283. Referring to claim 1, 3, 4, 22-23, Wiser discloses an online music distribution system wherein a client transmits encrypted user information (i.e. credit card number), over the Internet using SSL v3, to a media licensing center enable purchasing of media content (Col. 13, lines 16-27 & Col. 16, lines 53-65), which meets the limitation of receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device, the shared secret identifies a user, the shared secret is a credit card number. The user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client (Col. 19, lines 15-38), which meets the limitation of transmitting encrypted content via the insecure communications channel from a content server to the device, receiving a confirmation authorizing release of a decryption key, and sending the decryption key for decryption of the encrypted content, send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received, the confirmation is sent upon payment by a user of the device for the downloaded

content. Wiser does not specify that the media licensing center/merchant server transmits the credit card information to the payment processor over a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the elements of Figure 1B of Wiser to be connected using communications channels secured with physical protection measures in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]). Figure 1B shows a content server, a point of sale terminal, and a payment server. Figure 1A shows one or more remote devices.

Referring to claim 2, Wiser discloses that the user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client (Col. 19, lines 15-38), which meets the limitation of the confirmation is based on payment for the transmitted encrypted content.

Referring to claim 5, Wiser discloses that after transmission of the media content, which includes the media key, has completed, a notification is sent from the delivery system to the content manager (Col. 19, lines 44-49). Wiser does not disclose that the client sends a notification to the delivery system acknowledging completion of the media content download. However, Examiner takes OFFICIAL NOTICE that it is well known to those of ordinary skill in the art at the time the invention was made that when a download has complete, a notification is sent to acknowledge the download completion.

Referring to claim 6, Wiser discloses that the encrypted media/media key is sent via the Internet (Figure 9BA, 960), which meets the limitation of the decryption key is sent to the device via the insecure communication channel.

Referring to claim 7, Wiser discloses that the media key is sent to the delivery system from the content manager (Figure 9BA, 954). Wiser does not specify that the content manager and the delivery system are connected via a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the elements of Figure 1B of Wiser to be connected using communications channels secured with physical protection measures in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]).

Referring to claim 8, Wiser discloses that the client transmits a randomly generated receipt to a delivery system (Figure 9BA, 948 & Col. 8, lines 32-34), which meets the limitation of receiving a random plaintext from the device.

Referring to claim 9, Wiser discloses utilization of SSL v3 (Col. 6, lines 15-23). Examiner takes OFFICIAL NOTICE that it is well known in the art that SSL v3 utilizes shared secrets encoded by a hash function of a combination of the shared secret and the random plain text as claimed.

Referring to claim 10, Wiser discloses that the content key is encrypted (Figure 9BA, 954), which meets the limitation of encrypting the decryption key before sending it to the device.

Referring to claims 12, 14, Wiser discloses that after transmission of the media content, which includes the media key, has completed, a notification is sent from the delivery system to the content manager (Col. 19, lines 44-49). Wiser does not disclose that the client sends a notification to the delivery system acknowledging completion of the media content download. However, Examiner takes OFFICIAL NOTICE that it is well known to those of ordinary skill in

the art at the time the invention was made that when a download has complete, a notification is sent to acknowledge the download completion.

Referring to claims 13, 15, Wiser discloses utilization of SSL v3 (Col. 6, lines 15-23), therefore all transmissions would be protected using the SSL protocol which utilizes MD5 checksums for message authentication codes, which meets the limitation of the content download confirmation value is based on an MD5 checksum, receiving a random plaintext from the device, receiving a hash of the shared secret and the random plaintext for each shared secret, computing a hash of the shared secret with the random plaintext to produce a cyphertext for each shared secret, comparing the cyphertext to each of the received hash of each of the shared secrets, and in the case of a match, identifying the corresponding transmitted encoded content, encoding a content download confirmation value for the transmitted encoded content using the shared secret, and comparing the computed content download confirmation value to the received content download confirmation value to verify a complete content download.

Referring to claim 16, Wiser discloses that the client can receive the content prior to purchasing (Col. 16, lines 4-40), which meets the limitation of after verification of the complete content download, causing a prompt to be sent to a user of the device to purchase the downloaded content, and receiving a confirmation of receipt of payment.

Referring to claim 17, Wiser discloses that the content is encrypted prior to being downloaded (Col. 19, lines 15-38), which meets the limitation of content stored in the content server is encrypted prior to a start of a download process.

Claims 20, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser, U.S. Patent No. 6,385,596, in view of Parenty, U.S. Publication No. 2002/0064283, and further in

view of Katayama, U.S. Publication No. 2002/0027994. Referring to claims 20, 26, Wiser discloses an online music distribution system wherein a client transmits encrypted user information (i.e. credit card number), over the Internet using SSL v3, to a media licensing center enable purchasing of media content (Col. 13, lines 16-27 & Col. 16, lines 53-65), which meets the limitation of receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device, the shared secret identifies a user, the shared secret is a credit card number. The user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client (Col. 19, lines 15-38), which meets the limitation of transmitting encrypted content via the insecure communications channel from a content server to the device, receiving a confirmation authorizing release of a decryption key, and sending the decryption key for decryption of the encrypted content, send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received, the confirmation is sent upon payment by a user of the device for the downloaded content. Wiser does not specify that the media licensing center/merchant server transmits the credit card information to the payment processor over a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the elements of Figure 1B of Wiser to be connected using communications channels secured with physical protection measures in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]). Figure 1B shows a content server, a point of sale terminal, and a payment server. Figure 1A shows one or more remote devices. Wiser does not disclose that the content key is sent to the user after the encrypted content has been downloaded

and in response to an acceptance of terms. Katayama discloses that the content key is sent to the user after the encrypted content has been downloaded and in response to a purchase order for the content key ([0064] & [0078]), which meets the limitation of after receiving the confirmation of successful encrypted content download from the content server, prompting the user to accept terms of download and decryption of the encrypted content, after receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the encrypted content of Wiser to include a trial portion as discussed in Katayama such that a purchase order is required by the user to access the high quality version of the content, in order to provide users a chance to sample the audio content before deciding whether to purchase the audio content while providing content providers a means to prevent illegal use and illegal copying of high sound quality audio contents as taught by Katayama ([0009] & [0089]).

(10) Response to Argument

Appellant argues, "Wiser in view of Parenty fails to teach of suggest receiving a shared secret via an insecure channel." This argument is not persuasive because Wiser discloses an online music distribution system wherein a client transmits encrypted user information (i.e. credit card number), over the Internet using SSL v3, to a media licensing center enable purchasing of media content (Col. 13, lines 16-27 & Col. 16, lines 53-65), wherein the user information represents the shared secret and the Internet represents the insecure channel.

Appellant argues, "SSL is a secure channel and not an insecure channel…the Examiner fails to recognize that use of SSL with any channel on the Internet makes the channel secure."

This argument is not persuasive because SSL is a protocol, and not a channel. Therefore, Wiser discloses securely distributing user information over an insecure channel.

Appellant argues, "Wiser in view of Parenty fails to teach or suggest receiving a shared secret twice, but in two forms, *i.e.*, an encoded form and a plain text form…neither Wiser nor Parenty singly or in combination teach or suggest a media licensing center receiving the credit card information twice, but in two different forms." In response, it is noted that the features upon which applicant relies (i.e., receiving a shared secret twice at the same device) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Wiser in view of Parenty shows a media licensing center receiving encrypted user information (i.e. credit card number) for a client (Wiser: Col. 13, lines 16-27 & Col. 16, lines 53-65). The media licensing center then transmits the credit card number to the payment processor (Wiser: Figure 6A, step 612). Parenty provides a motivation of why it would have been obvious to one skilled in the art at the time of the invention for this transmission to occur over a secure channel (i.e. a hard wired channel) in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]). Therefore, the media licensing center would receive the credit card information in an encrypted form, while the payment processor would receive the credit card information in a non-encrypted form.

Appellant argues, "It would not have been obvious to combine the purchase of the second key of Katayama with Wiser, because in Wiser, the media file is already purchased prior to

sending the media file…there would be not reason to purchase the media file again in Wiser." This argument is not persuasive because in the proposed modification, the purchase order would not be transmitted until after the media file was received. Specifically the motivation states that it would have been obvious to one of ordinary skill in the art at the time the invention was made for the encrypted content of Wiser to include a trial portion as discussed in Katayama such that a purchase order is required by the user to access the high quality version of the content, in order to provide users a chance to sample the audio content before deciding whether to purchase the audio content while providing content providers a means to prevent illegal use and illegal copying of high sound quality audio contents as taught by Katayama ([0009] & [0089]).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Conferees:

/Jung Kim/
Primary Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432